

Cyber Early Warning System on Security Operations Center

Timo Koskimäki¹, Jouni Pöyhönen¹, Martti Lehto¹ and Mika Hållfast²

¹University of Jyväskylä, Finland

²DNV Cyber, Espoo, Finland

timo.a.koskimaki@jyu.fi

jouni.a.poyhonen@jyu.fi

martti.j.lehto@jyu.fi

mika.hallfast@dnv.com

Abstract: An Early Warning System (EWS) is a framework or collection of tools developed to identify and deliver timely alerts about potential threats, risks, or adverse events across various situations. Its main objective is to support decision-makers in implementing preventive actions that reduce the impact of possible hazards or disasters, thereby protecting lives and resources. Modern digital society depends on the interconnection and collaboration of essential infrastructures, which require adequate situational awareness (SA) to manage growing cyber risks. In the cyber domain, a key priority is safeguarding critical infrastructure (CI) against threats amid a surge in both the frequency and sophistication of cyberattacks. These evolving attacks allow adversaries to disrupt vital services remotely, creating significant risks and uncertainty in the absence of adequate SA and thus protection. The Cyber Early Warning System (CEWS) is essential within the cyber domain, integrating for example artificial intelligence (AI) to introduce a new approach to early warning capabilities. As a component of the cyber threat intelligence (CTI) process, CEWS offers an innovative methodological framework for navigating and operating in today's complex cyber environment. In large networked systems, CEWS gathers and correlates heterogeneous information from multiple sources, delivering timely and actionable insights to help prevent or mitigate potential risks by supporting effectively an organization's SA. Security Operations Center (SOC) is a key element to protect an organization's digital assets by continuously monitoring, detecting, investigating, and responding to cyber threats. The SOC is an essential part of an organization's SA and risk management, as it particularly supports risk identification, monitoring, and control by continuously providing information to detect, assess, and manage cybersecurity risks. This paper highlights the importance of collaborating with the Cyber Early Warning System and the Security Operations Center.

Keywords: Organization, Cyber early warning, Security operations center, Risks assessment

1. Introduction

Modern society depends on the coordinated, reliable performance of many critical infrastructure (CI) organizations, whose collective success increasingly relies on a resilient national system-of-systems. Because today's digital environment is tightly interconnected, organizations must maintain real-time situational awareness (SA) of cyber threats to manage growing risks to their assets. As cyberattacks become more frequent and sophisticated, protecting essential organizations has become a top priority. These evolving threats allow adversaries to remotely disrupt vital services, heightening risks and uncertainty, especially when organizations lack sufficient SA and the safeguards needed to support effective risk assessment.

Throughout history, societies have developed early warning systems to detect and respond to threats. Prior to modern technology, cities relied on external outposts to identify and signal approaching dangers. Today, states employ advanced surveillance systems, including radar and satellite technologies, to continuously monitor their borders and environments. These systems enable timely detection of emerging threats and facilitate appropriate defensive responses. An Early Warning System (EWS) refers to a set of tools or mechanisms designed to identify potential risks and provide timely information, supporting decision-makers in implementing preventive measures to mitigate impacts and protect lives and resources (Ultimaco, 2025).

Today a Cyber Early Warning System (CEWS) is needed in the context of the cyber domain. It incorporates artificial intelligence elements to enable a new approach to early warning capability. CEWS is part of the cyber threat intelligence process and provides a new methodological framework for operating in a complex cyber environment.

According to the EU NIS2 Directive, "essential and important entities should take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services" (EU, 2023). Identifying cyberattacks are increasingly difficult, and the fast-changing nature of cyber environment demands both agility and preparedness for unforeseen threats. While risk assessment methods can address most known and partially known events, completely unknown threats require alternative approaches.

The definition of the research problem emphasizes the challenges of proactively identifying unknown risks that threaten an organization's cybersecurity and leveraging that information within operational processes. In this sense, CEWS is needed to develop an extended approach for providing better CTI to support an organization's operational purposes in a complex cyber environment. It is an important threat-intelligence process, particularly for identifying unknown threats and enhancing situational awareness in organizational risk-assessment activities. In many cases, these unknown threats are associated with dark-web entities.

Threats are characterized by the motivation and capabilities of threat actors. For example, such attributes are not directly observable within traditional risk assessment processes, particularly in environments such as the dark web. This information can, however, be inferred from multiple sources using CEWS and by leveraging advanced technologies, such as Artificial Intelligence (AI). The aim of this study is to evaluate the applicability of such information across different stages of the Security Operations Center (SOC) process, and thereby as part of an organization's overall risk assessment.

SOC forms the operational core of an organization's cyber defense capability. It is mainly reactive element, because its purpose is to detect, investigate, and respond to security incidents. A SOC is more than just a 'technical monitoring center'; it is an integral part of an organization's real-time situation awareness tool and part of overall risk management strategy. It plays a key role in two main areas: identifying and monitoring risks and managing and responding to them effectively. In this role, the SOC relies on relevant CI to guide its actions. An effective CEWS is a key element in building that awareness and, consequently, an integral part of the organization's overall robust risk management process. This paper outlines the structural domains of SOC, from strategic steering to proactive prevention, describing how each contributes to the overall life cycle of threat management and operational assurance. The model presented here is designed to be framework-agnostic, scalable, and suitable as a foundation for further research and capability development.

In this paper, we examine the importance of a Cyber Early Warning System (CEWS) as part of Security Operations Center (SOC) operations. The paper emphasizes the importance of CEWS data for the SOC process at different stages in order to manage unknown risks proactively. Technically, CEWS data can be integrated with the SOC's Security Information and Event Management (SIEM) system. The research framework outlines the structure of risk categorization, while the empirical part focuses on the SOC process. The main question is:

'What are the key elements for the cooperation between CEWS and SOC in risks identification?'

2. Cyber Security Situational Awareness

Cybersecurity situational awareness is the real-time understanding of the digital environment, including emerging threats, vulnerabilities, and the potential impact of attacks, to enable timely and effective responses. It involves perceiving events, comprehending their significance, and projecting potential future scenarios. Achieving this requires robust data collection, advanced analytics, and effective information sharing.

There are three key components to creating a situational picture: (Endsley, 1995)

- Perception of the elements in the environment
- *The goal is to perceive the status, attributes, and dynamics of relevant elements in the environment.*
- Comprehension of the situation
- *This involves a synthesis of elements through the processes of pattern recognition, interpretation, and evaluation.*
- Projection of future status
- *This involves the ability to project the future actions of the elements in the environment.*

In his article "Flow Analytics for Cyber Situational Awareness", Sid Faber considers measures to develop situational awareness in both public and private organizations to be among the most significant near-term objectives for improving cybersecurity. Faber recommends applying the framework developed by Endsley to the monitoring requirements of the cyber operational environment. (Faber, 2015)

3. Risk Categorization as a Research Framework

Effective risk assessment requires systematically collecting and analyzing data while accounting for evolving threats and vulnerabilities. It helps raise awareness, prioritize early warning systems, and guide disaster prevention and response.

Risk knowledge depends on an up-to-date understanding of the cyber environment, including current events and changing threat actors. Since these changes happen quickly, maintaining continuous situational awareness is essential.

Threats can be categorized as immediate (e.g., ongoing cyberattacks on critical infrastructure) or long-term (e.g., geopolitical risks). Managing cyber risk relies on accurate awareness of risks and impacts. While more information improves risk management, unknown risks (“unknown unknowns”) remain difficult to predict and are often outside traditional risk planning.

Figure 1 shows a schematic structure of risk categorization. In this table, the model categorizes events by “identification” and “accuracy of knowledge or certainty”. (Kim, 2012, mod)

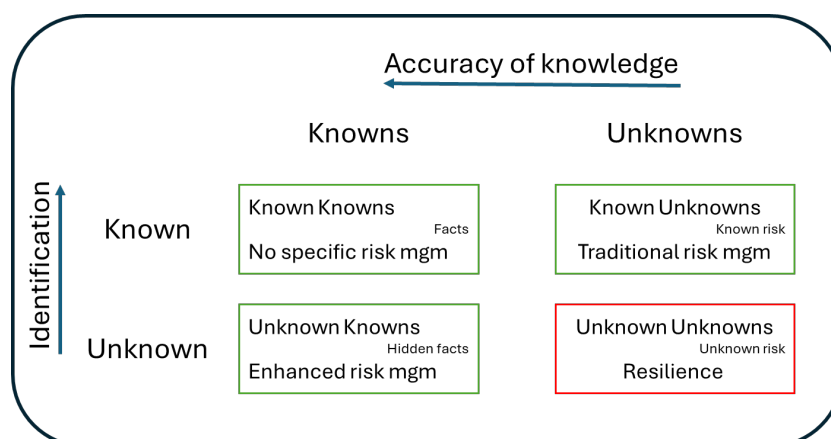


Figure 1: Schematic structure of modified risk categorization

The first three categories of events (known knowns, known unknowns, and unknown knowns) can be addressed through established risk assessment methods and processes. However, completely unknown possibilities require a different approach. To address these, organizations must enhance the overall resilience of their business operations, for example by implementing a Cyber Early Warning System (CEWS) integrated with Security Operations Center (SOC) activities.

4. Early Warning System

Early warning systems (EWS) are essential for example climate action because they provide timely alerts about hazards such as floods, droughts, and wildfires, helping save lives and reduce damage. Despite global progress, challenges like limited funding, data gaps, and communication issues remain, requiring continued cooperation. For long-term effectiveness, these systems must be continuously maintained and improved. The Third International Conference on Early Warning (2006) produced a practical checklist under the Hyogo Framework for action, outlining four key components of effective, people-centered early warning systems to help governments and communities strengthen disaster risk reduction (Figure 2). (ISDR, 2006)

EWS is a key tool that alert communities to hazards, giving time to prepare. They must be adaptable, regularly updated, and upgraded. Using tech like machine learning, data analytics, and advanced environmental monitoring improves warning accuracy and speed. Ongoing maintenance and enhancements are essential for EWS to remain effective and sustainable. (Sakaloukaya, 2024)



Figure 2: Four key elements of an early warning system

An effective EWS requires timely, clear, and unambiguous communication of information, while accounting for recipients' capacity to interpret and act on alerts. Warnings must be accurate and actionable, with thresholds calibrated to avoid both alert fatigue and insufficient notification. Additionally, information should be tailored to different decision-making levels.

For early warnings to support system defense, recipients must have predefined procedures, methods, and automation in place to process alerts efficiently. They must also understand EWS's operational logic, terminology, and resources, and be able to critically apply its outputs to protect the system.

In cyberdomain, Cyber Early Warning System's (CEWS) main focus is to give key information to decision makers and security teams about emerging threats before they happen. By having that information and using it appropriately in the decision-making process, it is possible to prevent the oncoming attacks at the early stage. EWS in cyber domain is a system or process of collecting and analyzing data from all layers of internet, surface web, deep web and dark web. By collecting and analysing the data it is possible to gather cyber threat information (CTI) of emerging cyber threats. By getting information about emerging cyber threats, it is possible to start preventive measures to defend against attacks before they reach the protected system or even occur in first place. CEWS is situated to work before attack triggers traditional indicators like Indicator of Compromise (IoC). Those early signals can be for example data found from data leaks, new tactics, techniques, and procedures (TTP's) of threat actors, new vulnerability in the system, device or protocol in use, discussions about protected organization in various darkforums, geopolitical events, and for example attacks occurring in the same region, operating sector, organizations supply chain, or for example against same field of political thinking.

Regarding the future development of CEWS, the primary focus will be on identifying an appropriate baseline model for performance evaluation and on developing an automated method to determine the date when a cyber threat becomes publicly known. Additionally, the method will undergo continuous refinement to enable the generation of more detailed and informative alerts. Future iterations will also incorporate a Natural Language Processing (NLP) component aimed at extracting relevant knowledge and insights from network posts that reference the identified terms. (Sapienza & al., 2017)

By implementing automating technologies and methods such as Large Language Models (LLMs), Machine Learning (ML) and Natural Language Processing (NLP) to CEWS, it is possible to utilize the enormous amount of information that internet provides in a rapidly changing environment. It is not possible to go through this information manually and find key information about early warning signals from multiple large scaling sources. In Figure 2 we show the flowchart from the initial sources of information to the cyber early warning signal and until receiving and reacting to that information.

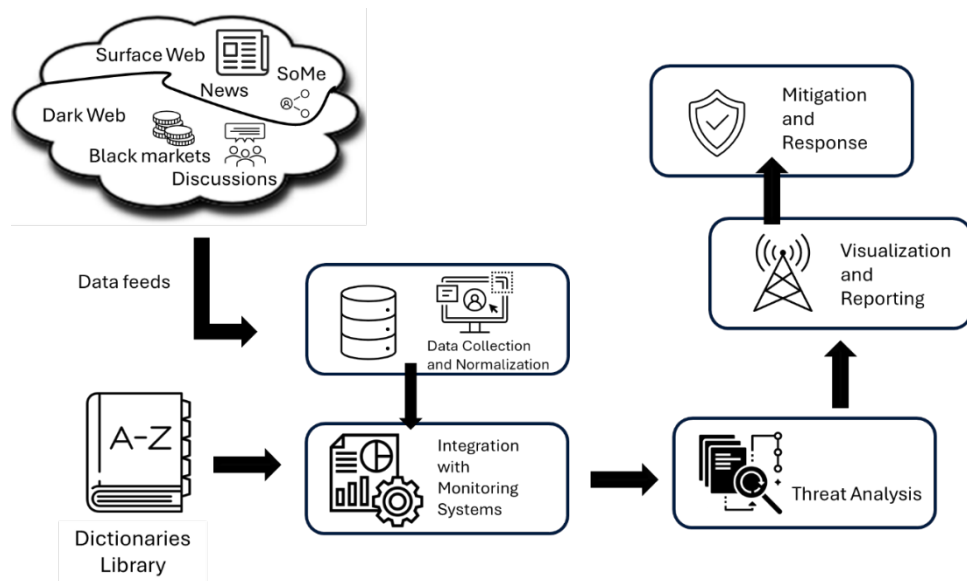


Figure 3: Cyber Early Warning System (CEWS)

Process starts with the dataset. There are enormous amounts of data that can be collected from different layers of internet. Data consists of, for example Surface Web's different news pages and social media sites or Dark Web's different black markets and discussion forums. The data is then collected and normalized and added to monitoring system. According to the needs of the operating environment, various dictionary-like filters are defined, which are used to collect essential information from the data for analysis. The material that passes through the filters is analysed and various risk assessments are made based on the analysis. This information is compiled into an easy-to-understand report. Based on that report defensive measures can be adjusted, and risks can be mitigated.

5. Cyber-physical Environment

The cyber-physical environment combines physical reality and digital technologies through various networking methods. The most extensive and comprehensive solution is the internet. With internet networking solutions it is possible to connect physical processing tools to systems anywhere in the world with internet connectivity.

The Internet consists of three different layers: the surface web, the deep web, and the dark web. Each of these has its own role and characteristics with the content and purpose of the network (Lehto & Koskimäki, 2025). This knowledge of the different levels of the network is important, since the Cyber Early Warning System (CEWS) model, collects data from these different levels of the network.

Surface Web

The surface web, i.e. the visible web, is the top layer of the internet that can be accessed using regular web browsers (Khera, 2020). The surface web is the part of the internet that is openly available and easily accessible to all internet users. It is indexed by search engines and easily searchable through various search engines. Using surface web with default settings and browsers, without for example VPNs, leave trace from user, for example users IP-address and cookies collected by websites and internet services. (Varma, 2018)

Deep Web

Although the deep web may seem obscure, people use it constantly. Activities like email, private messaging, online banking, and accessing subscriber-only news all rely on it. (Vienažindytė, 2021) The deep web consists of online content that search engines cannot index, such as internal organizational databases, paywalled material, dynamically generated pages, and content accessible only through a site's own search tools. (Hatta, 2020) Estimates over the years have shown that the deep web is vastly larger than the surface web, making up most of all online information. Because the internet contains an enormous and ever-changing volume of data, the exact proportion between the surface web and deep web cannot be precisely measured, but most online content belongs to the deep web. (Finklea, 2017)

Dark Web

The dark web is a hidden section of the internet that cannot be accessed with standard surface web browsers. It enables users to remain almost entirely anonymous by encrypting data and sending it through multiple network nodes. In practice, a dark web user's traffic is routed through the network terminals of many other users, making it extremely difficult or impossible to identify the original source of the network traffic. This layered routing system is known as the "onion network," reflecting its multiple levels of encryption. The strong anonymity it offers draws people who want to keep their activities concealed. In the first hand, dark web was used by journalists and freedom activists of the authoritarian states. The dark web is nowadays known for its illegal marketplaces, the distribution of harmful or forbidden content, cybercriminal and espionage networks among other illicit activities. (Chertoff & Simon, 2015)

6. Security Operations Center

This chapter describes the core structural domains of a Security Operations Center (SOC), ranging from strategic oversight to proactive threat prevention, and explains how each domain supports the full lifecycle of threat management and operational assurance. The proposed process model is framework-agnostic, scalable, and intended to serve as a foundation for future research and capability development. A SOC forms the operational core of an organization's cyber defense capability. Its purpose is to detect, investigate, and respond to security incidents while continuously improving the organization's situational awareness and resilience. SOC functionality includes both process and technical components. According to our research, the appropriate structural process elements are as follows:

Steering

Steering function defines the mechanisms through which a Security Operations Center (SOC) aligns its activities with an organization's overarching risk management objectives. Effective steering is characterized by a deliberate balance between situational awareness and operational performance. Fundamentally, steering governs the allocation and coordination of the three core resources underpinning any security capability: people, processes, and tools. Through this governance, steering enables the transformation of the SOC from a primarily reactive technical function into a structured, managed capability that contributes directly to the organization's resilience and its strategic risk posture.

Visibility

Visibility constitutes the foundational element of all Security Operations Center (SOC) activities. It reflects the SOC's capacity to observe, understand, collect and store event information occurring within an organization's digital environment. This capability is fundamentally data-driven, relying on the continuous and voluminous streams of telemetry generated by organizational assets, systems, and services during normal operation. SOC visibility is derived from three primary sources. First, transactional data, which is obtained from telemetry and event logs, provides detailed records of system and user activity. Second, threat intelligence supplies awareness of external threats and adversarial behaviours relevant to the organization. Third, contextual information describes the organization's assets, configurations, and established patterns of normal behaviour, enabling meaningful interpretation of observed events. Collectively, these sources of visibility support both detection and decision-making within the SOC. Visibility functions as the analytical lens through which the SOC interprets its operational environment and identifies indicators of compromise. In the absence of sufficient visibility, neither proactive threat hunting nor effective reactive defence can be achieved.

Detection

Detection serves as the mechanism through which visibility is transformed into actionable security intelligence. It defines how a Security Operations Center (SOC) identifies potential security anomalies within an organization's monitored environment. Detection techniques range from basic anomaly-based alerting to advanced, context-aware rules that correlate multiple events across diverse data sources. Enrichment processes further enhance detection by adding contextual information to raw event data, thereby improving analytical accuracy and reducing the incidence of false positives. The output of the detection function is a set of findings that merit deeper examination during the investigation phase. The quality of these findings directly influences the overall efficiency of the SOC, as well-calibrated detection mechanisms reduce analytical noise and enable faster, more confident response actions. In this regard, detection constitutes both a technical and analytical capability, converting raw telemetry into meaningful security awareness.

Investigation

Investigation is the systematic process of validating, contextualizing, and interpreting detected anomalies. Its primary objective is to ascertain whether an event constitutes a genuine threat and to determine the appropriate course of action. Effective investigation relies on the capacity to correlate information from diverse data sources, employ suitable analytical tools, and integrate both automated processes and experts' analysis.

The investigation process aims to construct a structured understanding of:

- The nature and intent of the identified threat or anomaly
- The assets and systems affected
- The behavioral of the anomaly to these assets
- The potential or necessary remediation measures

Ultimately, investigation serves as the mechanism by which raw data is transformed into actionable knowledge. It converts signals into insight and insight into informed decisions, functioning as the pivotal link between detection and response.

React

The react function is responsible for addressing security events that require immediate containment or mitigation. It demonstrates the Security Operations Center's (SOC) ability to respond swiftly and decisively once a validated threat is identified. Typical reactive measures include isolating affected systems, blocking malicious connections, and initiating predefined remediation protocols. The effectiveness of the reaction phase is measured by its ability to limit damage and prevent escalation. By minimizing the interval between detection and containment, the SOC ensures operational continuity and reduces potential business impact.

Respond and Recover

The respond and recover domain encompasses structured activities aimed at restoring normal operations following an incident. While reaction primarily focuses on immediate containment, the response and recovery phase addresses the broader processes of resolution, remediation, and organizational learning. This phase incorporates coordinated incident response, forensic analysis, business continuity measures, and executing recovery, based on established recovery plans. Collectively, these functions ensure that technical restoration, organizational communication, and procedural follow-up are executed in a controlled, systematic, and well-documented manner.

Prevent

The prevention function is primarily concerned with minimizing exposure to prospective threats by mitigating vulnerabilities identified through prior Security Operations Center (SOC) processes. Preventive measures may encompass patch and configuration management, architectural modifications, user awareness programs, and the automation of system hardening procedures. These activities aim to reduce the attack surface and remediate known vulnerabilities before they can be exploited. By systematically leveraging SOC findings and operational observations, the prevention function effectively closes the feedback loop, ensuring that each security incident informs strategies that enhance the overall resilience and security posture of the organization.

Co-operation on Cyber Early Warning System and the Security Operations Center

In this chapter, CEWS data are linked to the empirically defined SOC process of the study. Drawing on the study's theoretical framework, the different phases of the SOC process outlined above benefit from early warning information, thereby facilitating proactive risk identification in so-called 'unknown unknown' situations.

Cyber Early Warning System (CEWS) is a value-adding piece to a workflow of Security Operation Center (SOC). In SOC environment the earlier coming attack is detected and the earlier it is mitigated, less resources are consumed at the defense against those attacks becomes. It is therefore important to prevent these attacks from materializing in first place. Any help for preventing the attack firsthand helps the workload of SOC. There should not be any overlapping between CEWS and SOC tasks, but merely CEWS should increase the SOC ability to proactively defend against different kinds of cyber-attacks. That is why CEWS must be integrated into each SOC environment in a way that is suitable for it and perform tasks that support the operation of the SOC, not to replace its different functions.

CEWS information can enhance every stage of the SOC process. Steering involves directing the SOC's capabilities at both operational and strategic levels, guided by CEWS insights. This information helps align SOC activities with

the evolving threat landscape. With CEWS information SOC can have more information on the development of the threat field and the prevailing state in the cyber operations environment. In this context, early warning information is wider scoped and aggregated information about actors and their TTP's in the cyber environment, ongoing phenomena, development trajectories of different subjects and for example early-stage warnings about dark market products, datasets or attack orders.

CEWS shapes the SOC's scope of visibility by prioritizing monitoring on critical areas or assets, while also complementing the SOC's internal threat intelligence. CEWS would increase the visibility of the SOC by producing cyber situational awareness and cyber threat intelligence outside the SOC environment. CEWS could also bring together situational awareness produced by itself, industries and experts in a similar way to, for example, sector-specific information sharing and collaboration network ISAC (Information Sharing and Analysis Center).

For detection, CEWS provides indicators of tactics, techniques, and procedures (TTPs), allowing detection rules to be fine-tuned for greater sensitivity and alignment with operational processes.

Investigation enables CEWS to remain viable despite imperfect accuracy by providing process-driven validation of weak signals. During this phase of the process, CEWS clarifies, for instance, the tools and methods commonly used by specific threat actors. In security analysis, the information is further enriched to anticipate potential developments.

CEWS also drives capability development, offering advanced insights that help evolve SOC operating models and response practices.

In the respond, recovery and preventing phases, CEWS enables organizations to effectively practice receiving and acting on early warning information. The Prevent phase emphasizes proactive measures, such as segmentation and other controls, where early CEWS alerts allow preventive actions that can stop attacks before they occur.

Although an organization's SOC primarily concentrates on operational and tactical activities to maintain cybersecurity situational awareness, an early warning system can also deliver strategic-level insights that support decision-making, particularly by enabling a deeper understanding of trend-based threat intelligence. A CEWS can direct SOC analysts' attention to specific areas of concern when it identifies correlations between the defended network and ongoing attack campaigns targeting a particular industry, supply chain, or similar context. Furthermore, a CEWS can help the SOC adapt its sensors and detection mechanisms to the tactics, techniques, and procedures of malicious actors, increasing sensitivity to relevant threats and improving the ability to detect and defend against such activities.

7. Conclusion

The cyber-physical environment integrates physical systems with digital technologies through networking, most notably the internet, which enables global connectivity of physical and digital systems. The internet is divided into the surface web, deep web, and dark web, each serving different purposes. Understanding these layers is important, as the Cyber Early Warning System (CEWS) collects data from all three.

It is important that an organization's situational awareness includes identifying critical digital elements within the environment, interpreting their significance, and understanding how they interrelate in the context of information security. It also involves anticipating future conditions and potential threats based on current data, enabling proactive rather than reactive responses. In this context, CEWS serves as a proactive cybersecurity capability designed to detect threats before, or at the earliest stages of an attack, allowing organizations to respond before substantial harm occurs. Unlike traditional security tools that generate alerts only once an attack is underway, CEWS focuses on identifying early indicators and conditions that could lead to future attacks. As a result, it is a vital component of an organization's Security Operations Center (SOC), enhancing situational awareness and supporting more effective risk assessment, particularly in complex and highly uncertain "unknown-unknown" cyber environments.

CEWS enhances all stages of the SOC process by aligning operations with the evolving threat landscape. The following phases of the SOC process have been identified: Steering, Visibility, Detection, Investigation, React, and Respond & Recover. SOC guides strategic and operational steering, focuses visibility on critical assets, and strengthens threat intelligence. CEWS improves detection through refined tactics, techniques, and procedures-based indicators, supports investigations by clarifying threat actor behaviours, and enriches security analysis to anticipate future risks. It also drives capability development and enables proactive response, recovery, and prevention by supporting early warning-driven actions that can stop attacks before they occur.

The SOC process of the study can be conceptualized as comprising the aforementioned components, each with a distinct role. These roles correspond to the “key elements” identified in the research question and are essential for supporting the use of CEWS information within the context defined by the study’s framework.

In future work, our CEWS research team will focus on developing its early warning features. By integrating automated technologies such as Large Language Models (LLMs), Machine Learning (ML), and Natural Language Processing (NLP), CEWS can better leverage the vast amount of internet data in a rapidly changing environment. Manual analysis of this large-scale, multi-source information is not feasible for identifying early warning signals.

Ethics Statement: Ethical clearance was not required for the research

AI Statement: Ai tools have not been used in this research

References

- Chertoff, M. & Simon T. (2015). The impact of the dark web on internet governance and cyber security, Centre for International Governance Innovation and the Royal Institute for International Affairs, paper series: NO. 6, Feb 2015.
- Endsley M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors Journal* 37(1), 32-64.
- EU, (2023). NIS2 Directive (Directive (EU) 2022/2555)
- Faber, S. (2015). Flow Analytics for Cyber Situational Awareness. SEI Blog. (Retrieved 1/2026)
https://insights.sei.cmu.edu/sei_blog/2015/12/flow-analytics-for-cyber-situational-awareness.html
- Finklea K. (2017). Dark Web, Congressional Research Service, March 10, 2017
- Hatta M. (2020). Deep web, dark net: A taxonomy of “hidden” Internet. *Annals of Business Administrative Science*, 19(6), 277–292.
- ISDR, (2006). Developing Early Warning Systems: A Checklist. EWC III Third International Conference on Early Warning From concept to action 27 – 29 March 2006, Bonn, Germany. (Retrieved 1/2026)
https://www.unisdr.org/files/608_10340.pdf
- Khera, V. (2020). The Web Layers: Introduction to Surface, Deep and Darknet. <https://cyberprotection-magazine.com/theweb-layers-introduction-to-surface-deep-and-darknet>
- Kim, S. D. 2012. Characterizing unknown unknowns. Paper presented at PMI Global Congress 2012—North America, Vancouver, British Columbia, Canada. Newtown Square, PA: Project Management Institute.
- Lehto, M., & Koskimäki, T. (2025). Cyber Threat Intelligence and IoCs and IoAs Search on the Dark Web. In C. Lipps, & B. Han (Eds.), *Proceedings of the 24th European Conference on Cyber Warfare and Security* (pp. 348-356). Academic Conferences International. *Proceedings of the European Conference on Cyber Warfare and Security*, 24.
<https://doi.org/10.34190/eccws.24.1.3420>
- Sakaloukaya, I. (2024). How early warning systems are saving lives in Central Asia. (Retrieved 1/2026)
<https://climatepromise.undp.org/news-and-stories/how-early-warning-systems-are-saving-lives-central-asia>
- Sapienza, A., Bessi, A., Damodaran, S., Shakarian, P., Lerman, K., & Ferrara, E. (2017). Early Warnings of Cyber Threats in Online Discussions. In 2017 IEEE International Conference on Data Mining Workshops (ICDMW) (pp. 667–674). IEEE Computer Society. <https://doi.org/10.1109/ICDMW.2017.94>
- Ultimaco. 2025. What is an Early Warning System? (Retrieved 1/2026). <https://utimaco.com/service/knowledge-base/emergency-communications-and-public-warnings/what-early-warning-system-0>
- Varma S. (2018). CISO Guide: Surface Web, Deep Web and Dark Web – Are they different?
<https://www.cisoplatfrom.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different>
- Vienäzindyté, I. (2021). Syväverkko: mikä on deep web ja minkälaisia vaaroja siihen liittyy? NordVPN, (Retrieved 1/2026)
<https://nordvpn.com/fi/blog/mika-on-deep-web/>